

**ANALISIS PERBANDINGAN TUNNEL VPN L2TP, PPTP,
SSTP, DAN OPENVPN BERBASIS MIKROTIK
MENGUNAKAN METODE QOS**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi *Informatika*



disusun oleh

YEREMIA ALALINTI

16.11.0788

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS PERBANDINGAN TUNNEL VPN L2TP, PPTP,
SSTP, DAN OPENVPN BERBASIS MIKROTIK
MENGUNAKAN METODE QOS**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi *Informatika*



disusun oleh

YEREMIA ALALINTI

16.11.0788

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS PERBANDINGAN TUNNEL VPN L2TP, PPTP, SSTP, DAN
OPENVPN BERBASIS MIKROTIK MENGGUNAKAN METODE
QOS**

yang disusun dan diajukan oleh

Yeremia Alalinti

16.11.0788

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 23 Juni 2023

Dosen Pembimbing,



Melwin Syafrizal S. Kom. M. Eng

NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS PERBANDINGAN TUNNEL VPN L2TP, PPTP,
SSTP, DAN OPENVPN BERBASIS MIKROTIK
MENGUNAKAN METODE QOS**

yang disusun dan diajukan oleh

Yeremia Alalinti

16.11.0788

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Maret 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Arifiyanto Hadinegoro, S.Kom, MT
NIK. 190302289

Eli Pujiastuti, M.Kom
NIK. 190302227

Melwin Syafrizal, S.Kom., M.Eng
NIK. 190302105

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Juni 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Yeremia Alalinti
NIM : 16.11.0788

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Perbandingan Tunnel VPN L2TP, PPTP, SSTP, dan OpenVPN Berbasis Mikrotik Menggunakan Metode QOS

Dosen Pembimbing : Melwin Syafrizal S.Kom., M,Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, Selasa 22 Maret 2022

Yang Menyatakan,



Yeremia Alalinti

HALAMAN PERSEMBAHAN

Segala puji Syukur bagi TUHAN Yang Maha Esa atas hidayah dan karunia-Nya sehingga saya dapat menyelesaikan skripsi saya dengan lancar dan sebaik-baiknya. Skripsi ini saya persembahkan untuk:

1. Ibu saya tercinta Senny Vasty Wakary dan Bapak saya Toni Alalinti serta adik Debora Natasya Alalinti. Yang selalu mendoakan, semangat, dan memberikan fasilitas yang saya butuhkan.
2. Terimakasih Kepada Bapak Melwin Syafrizal, S.Kom., M.Eng selaku dosen pembimbing saya yang baik dan sabar dalam membimbing saya serta memberikan saya arahan dalam menyelesaikan penyusunan skripsi ini.
3. Terimakasih kepada seluruh Dosen pengajar Teknik Komputer atas ilmu dan motivasi yang diberikan saya ingat terus.
4. Terimakasih kepada Sovie Marscu Trixiana, yang telah menjadi support system saya yang telah memberikan dorongan untuk menyelesaikan skripsi ini dan memberi masukan untuk melengkapi skripsi saya ini, juga selalu ada ketika saya membutuhkan dan mendengarkan saya disaat berkeluh kesah tentang dunia perskripsian ini.

KATA PENGANTAR

Puji dan syukur penulis haturkan kehadiran TUHAN Yang Maha Esa, karena berkat rahmat dan hidayah-Nya-lah saya dapat menyelesaikan skripsi saya, Skripsi ini dibuat untuk memenuhi tugas akhir perkuliahan dan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Strata 1. Selain itu, skripsi ini juga dibuat sebagai salah satu wujud implementasi dari ilmu yang didapatkan selama masa perkuliahan.

Skripsi ini tentunya tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini saya ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

- Bapak Hanif Al Fatta, S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom.
- Bapak Melwin Syafrizal S.Kom, M.Eng selaku dosen pembimbing penulis dalam menyelesaikan skripsi.
- Bapak Arifiyanto Hadinegoro, S.Kom, MT dan Ibu Eli Pujastuti, M.Kom yang telah menjadi penguji dalam ujian skripsi penulis.

Terimakasih penulis juga haturkan untuk semua pihak yang telah membantu peneliti dalam menyelesaikan skripsi ini yang tidak dapat peneliti sebutkan satu persatu. Akhir kata penulis menyadari bahwa tidak ada yang sempurna, penulis masih melakukan kesalahan dalam penyusunan skripsi. Oleh karena itu, penulis meminta maaf yang sedalam-dalamnya atas kesalahan yang dilakukan penulis. Saya berharap semoga Tuhan Yang Maha Esa mengaruniakan rahmat dan hidayah-Nya kepada mereka semua. Semoga skripsi ini dapat bermanfaat bagi kita semua.

Yogyakarta, 22 Maret 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	1
1.3 Batasan Masalah	2
1.4 Maksud dan Tujuan Penelitian	2
1.4.1 Maksud Penelitian.....	2
1.4.2 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Metode Penelitian.....	3
1.6.1 Metode Pengambilan Data.....	3
1.6.2 Metode Pengembangan Sistem	3
1.7 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
2.1 Tinjauan Pustaka.....	5
2.2 VPN (Virtual Private Network).....	8
2.2.1 Confidential (Kerahasiaan)	8
2.2.2 Data Integrity (Keutuhan Data)	8
2.2.3 <i>Origin Authentication</i> (Autentikasi Sumber).....	8
2.2.4 Tipe VPN (Virtual Private Network).....	9

2.2.5 SSTP	10
2.2.6 PPTP	10
2.2.7 L2TP	10
2.2.8 OpenVPN	10
2.2.9 Keamanan VPN	10
2.3 Cloud Computing	12
2.3.1 Karakteristik Cloud Computing	12
2.3.2 Layanan Cloud Computing	13
2.3.3 Model Penyebaran <i>Cloud Computing</i>	14
2.4 IP Address	15
2.5 QoS (Quality of Service)	15
2.5.1 Delay	16
2.5.2 Throughput	16
2.5.3 Jitter	17
2.5.4 Packet Loss	17
2.6 Metode Pengembangan	18
2.7 Wireshark	19
2.8 Mikrotik CHR	19
2.8.1 Spesifikasi Minimum	19
2.8.2 License Cloud Hosted Router	19
BAB III METODE PENELITIAN	23
3.1 Tinjauan Umum	23
3.2 Tahap Analisis	23
3.2.1 Analisis Masalah	23
3.2.2 Solusi Masalah	24
3.3 Alat dan Bahan Penelitian	24
3.4 Metode Penelitian	25
3.4.1 Flowchart Alur Penelitian	25
3.4.2 Flowchart Alur Kerja	26
3.5 Desain Topologi	26

BAB IV HASIL DAN PEMBAHASAN	29
4.1 Implementasi.....	29
4.1.1 Instalasi Mikrotik CHR.....	29
4.1.2 Instalasi VPN Server L2TP.....	36
4.1.3 Instalasi VPN Client-A L2TP	39
4.1.4 Instalasi VPN Client-B L2TP	40
4.1.5 Instalasi VPN PPTP Server.....	42
4.1.6 Instalasi VPN <i>Client-A</i> PPTP.....	45
4.1.7 Instalasi VPN Client-B PPTP	47
4.1.8 Instalasi VPN Server SSTP.....	48
4.1.9 Instalasi VPN Client-A SSTP	56
4.1.10 Instalasi VPN <i>Client-B</i>	58
4.1.11 Instalasi VPN Server OpenVPN	61
4.1.12 Instalasi <i>Client-A OpenVPN</i>	68
4.1.13 Instalasi VPN Client-B OpenVPN.....	70
4.2 Pengujian.....	73
4.2.1 Pengujian QOS (Quality of Service).....	73
BAB V PENUTUP	80
5.1 Kesimpulan	80
5.2 Saran	80
DAFTAR PUSTAKA	81

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka.....	6
Tabel 2.2 Delay	16
Tabel 2.3 Throughput.....	16
Tabel 2.4 Jitter	17
Tabel 2.5 Packet Loss	17
Tabel 2.6 License CHR.....	20
Tabel 3.1 Hardware.....	24
Tabel 3.2 Software	25
Tabel 3.3 IP Address.....	27
Tabel 4.1 Pengujian Throughput.....	73
Tabel 4.2 Pengujian Packet Loss	75
Tabel 4.3 Pengujian Delay	76
Tabel 4.4 Pengujian Jitter	77

DAFTAR GAMBAR

Gambar 4.1 Download RAW Disk Image Mikrotik CHR.....	29
Gambar 4.2 Login Neo Cloud.....	30
Gambar 4.3 Membuat image.....	30
Gambar 4.4 Membuat IP Address.....	31
Gambar 4.5 Membuat Router	31
Gambar 4.6 Menambahkan interface	32
Gambar 4.7 Menambahkan Rule Port TCP	32
Gambar 4.8 Menambahkan Rule Port UDP.....	33
Gambar 4.9 Membuat instance	33
Gambar 4.10 Memilih Boot Source	34
Gambar 4.11 Memilih Flavor Instance	34
Gambar 4.12 Memilih Flavor Instance	35
Gambar 4.13 Menginput Key Pair	35
Gambar 4.14 Allocate Floating IP	36
Gambar 4.15 Login Winbox	37
Gambar 4.16 Mengaktifkan L2TP	37
Gambar 4.17 Membuat Secrets Client A	38
Gambar 4.18 Membuat Secrets Client B	39
Gambar 4.19 List Static IP Route	39
Gambar 4.20 L2TP Client.....	40
Gambar 4.21 IP Static Route Client-A	40
Gambar 4.22 L2TP Client.....	41
Gambar 4.23 IP Static Router	41
Gambar 4.24 Login Winbox	42
Gambar 4.25 Mengaktifkan PPTP Server.....	43
Gambar 4.26 Client-A Secrets	43
Gambar 4.27 Client-B Secrets	44
Gambar 4.28 Static IP Route	45
Gambar 4.29 PPTP Client-A.....	46

Gambar 4.30 PPTP Client-A.....	46
Gambar 4.31 PTP Client-B	47
Gambar 4.32 IP Static Route	47
Gambar 4.33 Login Winbox	48
Gambar 4.34 Template Certificate.....	49
Gambar 4.35 Server Certificate	49
Gambar 4.36 Certificate Client-A.....	50
Gambar 4.37 Certificate Client-B	50
Gambar 4.38 CA Certificate Self Signing	51
Gambar 4.39 Server Certificate Self Signing	51
Gambar 4.40 Self Signing Client-A.....	51
Gambar 4.41 Self Signing Client-B	52
Gambar 4.42 Gambar 4.43 Server Certificate Trusted	52
Gambar 4.43 Client-A Certificate Trusted.....	52
Gambar 4.44 Client-B Certificate Trusted.....	52
Gambar 4.45 Export Mycertificate	52
Gambar 4.46 Export Client-A Certificate	53
Gambar 4.47 Export Client-B Certificate	53
Gambar 4.48 Mengaktifkan SSTP Server.....	53
Gambar 4.49 Secrets Client-A	54
Gambar 4.50 Secrets Client-B	55
Gambar 4.51 Static Route vpn server	55
Gambar 4.52 Import CA Certificate	56
Gambar 4.53 Import Client-A Certificate	57
Gambar 4.54 SSTP Client-A.....	57
Gambar 4.55 IP Static Route	58
Gambar 4.56 Import CA Certificate	59
Gambar 4.57 Import Client-B Certificate	59
Gambar 4.58 SSTP Client.....	60
Gambar 4.59 Static IP Route	61
Gambar 4.60 Login Winbox	61

Gambar 4.61 Template Certificate.....	62
Gambar 4.62 Server Certificate	62
Gambar 4.63 Certificate Client-A.....	63
Gambar 4.64 Certificate Client-B	63
Gambar 4.65 CA Certificate Self Signing	64
Gambar 4.66 Server Certificate Self Signing	64
Gambar 4.67 Self Signing Client-A.....	64
Gambar 4.68 Self Signing Client-.....	64
Gambar 4.69 Server Certificate Trusted	65
Gambar 4.70 Client-A Certificate Trusted.....	65
Gambar 4.71 Client-B Certificate Trusted.....	65
Gambar 4.72 Export Mycertificate	65
Gambar 4.73 Export Client-A Certificate.....	65
Gambar 4.74 Export Client-B Certificate	66
Gambar 4.75 OpenVPN Server.....	66
Gambar 4.76 Client-A Secret.....	67
Gambar 4.77 Client-B Secrets	67
Gambar 4.78 Static IP Route	68
Gambar 4.79 Import CA Certificate	68
Gambar 4.80 Import Client-A Certificate.....	69
Gambar 4.81 OpenVPN Client-A.....	69
Gambar 4.82 IP Static Routes	70
Gambar 4.83 Import CA Certificate	70
Gambar 4.84 Import Client-B Certificate	71
Gambar 4.85 OpenVPN Client-B	72
Gambar 4.86 Static IP Routes	72
Gambar 4.87 Grafik Pengujian Throughput	74
Gambar 4.88 Diagram Pengujian Packet Loss	75
Gambar 4.89 Diagram Pengujian Delay	77
Gambar 4.90 Diagram Pengujian Jitter.....	78

INTISARI

Jaringan internet sudah menjadi bagian penting dalam masyarakat. Jaringan internet sudah menjadi aktivitas kegiatan sehari-hari bagi setiap orang dalam menggunakan jaringan internet. Biasanya digunakan dalam surfing internet, atau mengirim data yang bersifat penting. Namun muncul permasalahan yang dimana pada saat menggunakan jaringan internet data yang kirim bisa dilihat atau diambil oleh seseorang yang tidak bertanggung jawab.

Virtual Private Network (VPN) merupakan teknologi jaringan yang menghubungkan dengan jaringan publik untuk dibuat menjadi secure atau aman. VPN biasanya digunakan untuk kebutuhan pribadi atau kebutuhan dalam sebuah instansi yang membutuhkan privacy dalam berkomunikasi atau mengirim sebuah data. Karena dengan menggunakan VPN, jaringan internet yang bersifat publik menjadi secure. VPN juga menambah kecepatan dalam mengakses jaringan internet.

Pada penelitian ini dilakukan perbandingan kinerja dari protokol VPN. VPN sendiri mempunyai protokol-protokol yaitu PPTP, SSTP, L2TP dan OpenVPN. Penulis akan melakukan perbandingan kualitas kinerja dari protokol VPN dengan memanfaatkan cloud computing sebagai server dan mengacu pada parameter QoS(Quality of Service) yaitu delay, throughput, packetloss, dan jitter . Pengujian kinerja dilakukan dengan menggunakan streaming dan download.

Kata kunci: *Internet, VPN, QoS, Cloud computing.*

ABSTRACT

The internet network has become an important part of society. The internet network has become a daily activity for everyone in using the internet network. Usually used in surfing the internet, or sending important data. However, a problem arises where when using the internet network the data sent can be seen or taken by someone who is not responsible.

Virtual Private Network (VPN) is a network technology that connects public networks to make them secure. VPN is usually used for personal needs or needs in an agency that requires privacy in communicating or sending data. Because by using a VPN, the public internet network becomes secure. VPN also increases the speed in accessing the internet network.

In this study, a comparison of the performance of the VPN protocol was carried out. VPN itself has protocols namely PPTP, SSTP, L2TP and OpenVPN. The author will compare the performance quality of the VPN protocol by utilizing cloud computing as a server and referring to the QoS (Quality of Service) parameters, namely delay, throughput, packet loss, and jitter. Performance testing is done by using streaming and downloading.

Keyword: *Internet, VPN, QoS, Cloud Computing.*